UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/854,101	05/11/2001	Hung-Yu Lin		7720

7590 11/17/2004

Mrs. Hung-Yu Lin
17983 Pueblo Vista Lane
San Diego, CA 92127

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	PAPER NUMBER
2137	9

DATE MAILED: 11/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/854,101	LIN, HUNG-YU	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *May 11, 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-15 are pending.

Drawings

2. The drawings are objected to because

Fig. 3, element 44 shows g.sub.x1.sub.y1||c should be "g.sub.x1.sub.y1||c1" according to the specifications.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

3. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

4. The abstract of the disclosure is objected to because it does not include both embodiments, the first one with two proxies and the second with one proxy.

Correction is required. See MPEP § 608.01(b).

Claim Objections

5. Claim 5 is objected to because of the following informalities:

"5;" should be "5."

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As to claim 1, "said session key" on line 21, page 14 lacks antecedent basis.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beller et al. (US 5,222,140) in view of Fox et al. (Security on the Move: Indirect Authentication Using Kerberos).

Beller discloses a cryptographic method utilizing public key cryptographic techniques for session key agreement and authentication in a portable communication system comprising portable telephone and the specific port control unit with which the

portable telephone is in communication (Fig. 1), which reads on the first and second communication locations and the composite Diffie-Hellman protocol being used between two communication entities for message encryption and key agreement and distribution (Fig. 4) which reads on the steps of generating the secret numbers, the ephemeral numbers and composite numbers.

Beller does not disclose the proxied services.

Fox discloses using proxies as mediating services to enable secure access to mobile computer users while minimizing the client side complexity that such secure access imposes (page 155, right column, 1.2 Proxied Services).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of proxies as intermediaries as Fox teaches, in the system of Beller so as to provide authentication and performing security computation protocols that the end-users lack adequate computation power, bandwidth or power supply.

10. Claims 2-9 and 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beller et al. (US 5,222,140) in view of Fox et al. (Security on the Move: Indirect Authentication Using Kerberos) and further in view of Schneier (Applied Cryptography).

a) As to claims 2-3, 4-5 and 15, Beller and Fox do not disclose computing modulo P in a Galois field and raising the numbers to integer exponents.

Schneier discloses computing in a Galois field and raising the numbers to integer exponents (pages 254-255).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of Galois field and raising the numbers to integer exponents in the system of Beller and Fox, as Schneier teaches, so as to make the key is more complex and harder to break.

b) As to claims 6-9 and 12-14, Beller discloses authenticating portable phone identity (Fig. 2), however he does not disclose mutual authentication (challenge/response protocol).

Schneier discloses mutual authentication between two parties where challenges being exchanged (pages 54-55).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of exchanging challenges between communication parties as Schneier teaches, in the system of Beller and Fox, so as to authenticate all involved parties in a communication system.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
11/8/04

Andrew Caldwell
Andrew Caldwell